(19) Bureau voor de Industriële Eigendom Nederland

(11) 1005523

(12) C OCTROOI[20]

(21) Aanvrage om octrooi: 1005523

(22) Ingediend: 13.03.97

(51) Int.Cl.[6]
H04K1/00, H04L9/00, H04B1/69, H04N7/167

(41) Ingeschreven:
15.09.98

(47) Dagtekening:
15.09.98

(45) Uitgegeven:
02.11.98 I.E. 98/11

(73) Octrooihouder(s):
Technische Universiteit Eindhoven te Eindhoven.

(72) Uitvinder(s):
Giok-Djan Khoe te Eindhoven
Robert Peter Christina Wolters te Montfort
Alfons Willy Leo Janssen te Utrecht

(74) Gemachtigde:
Ir. J.J.H. Van kan c.s. te 5600 AP Eindhoven.

(54) **Werkwijze en communicatiesysteem voor het in gedeeltelijk gecodeerde vorm overdragen van informatiesignalen.**

(57) Werkwijze en middelen voor het in een communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken, waarbij een informatiesignaal wordt gesplitst in een voor verwerking van het signaal relevant deel en een restdeel. Het relevante deel wordt in een veilig gecodeerde vorm en het restdeel wordt in ongecodeerde vorm via het communicatiesysteem overgedragen. Na het decoderen daarvan wordt een overgedragen relevant deel van een informatiesignaal met een bijbehorend overgedragen restdeel tot het oorspronkelijke informatiesignaal gereconstrueerd. Het te coderen relevante deel van het informatiesignaal wordt bij voorkeur onder toepassing van 'Code Division Multiple Access' (CDMA)-techniek gecodeerd overgedragen. Het communicatiesysteem kan een 'point-to-multipoint' signaaldistributienet omvatten, waarbij verschillende gebruikers gelijktijdig informatiesignalen kunnen ontvangen en/of verzenden, waaronder begrepen een 'Community Antenna TeleVision' (CATV)-net en distributienetten voor elektrische energie.

NL C 1005523

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekeningen.

Korte aanduiding: Werkwijze en communicatiesysteem voor het in gedeeltelijk gecodeerde vorm overdragen van informatiesignalen.

De uitvinding heeft betrekking op een werkwijze voor het in een communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken.

Veilige overdracht van data is een belangrijk aspect bij communicatie via een "point-to-multipoint"-signaaldistributienet, waarbij verschillende gebruikers gelijktijdig informatiesignalen kunnen ontvangen en/of verzenden, zoals een "Community Antenna TeleVision" (CATV)-net of distributienetten voor elektrische energie, waaronder begrepen distributienetten voor elektrische tractie.

Een netwerkbeheerder dient in staat te zijn de toegang tot het net te controleren en dient verder te kunnen verzekeren dat overgedragen informatiesignalen alleen kunnen worden ontvangen door de geadresseerde. Met ontvangen wordt in dit verband bedoeld dat de geadresseerde de inhoud van de betreffende informatiesignalen tot zich kan nemen.

Voor het in een signaaldistributienet veilig overdragen van informatiesignalen zijn een groot aantal coderingstechnieken bekend zoals bijvoorbeeld de "Rivest, Shamir, Aldehman" (RSA) en "Data encryption Standard" (DES) encryptie-algoritmes waarbij met codeersleutels wordt gewerkt. Het over te dragen informatiesignaal wordt dan in zijn geheel gecodeerd en via het signaaldistributienet overgedragen, waarbij alleen de ontvanger welke de voor het decoderen van het bericht benodigde sleutel kent, in staat is om de inhoud van het informatiesignaal tot zich te nemen.

De mate van beveiliging hangt naast het gekozen codeeralgoritme ook af van de lengte van de codeersleutel. In het bijzonder geldt dat bij relatief breedbandige informatiesignalen en bij relatief lange codeer- en decodeersleutels, er een aanzienlijke hoeveelheid tijd gemoeid kan zijn met het overdragen van informatiesignalen. In veel praktische toepassingen is een extra vertraging bij de overdracht van signalen echter niet gewenst.

Aan de uitvinding ligt daarom in eerste instantie de opgave ten grondslag een werkwijze aan te geven voor het in een

communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken met een gereduceerde invloed op de overdrachtssnelheid van informatiesignalen.

Volgens de uitvinding wordt dit daardoor bereikt dat een informatiesignaal wordt gesplitst in een voor verwerking van het signaal relevant deel en een restdeel, waarbij het relevante deel in een veilig gecodeerde vorm en het restdeel in ongecodeerde vorm via het communicatiesysteem worden overgedragen en dat een overgedragen relevant deel van een informatiesignaal wordt gedecodeerd en met een bijbehorend overgedragen restdeel tot het oorspronkelijke informatiesignaal wordt gereconstrueerd.

Aan de uitvinding ligt het inzicht ten grondslag dat, door het van een over te dragen informatiesignaal afsplitsen van een voor de verwerking van het signaal relevant deel, het resterende gedeelte onbruikbaar is geworden. Onder een 'voor verwerking relevant deel' van het signaal worden in dit verband één of meer delen van een signaal begrepen waarmee, bij het ontbreken hiervan, de informatie in het restdeel niet meer kan worden herkend dan wel dat door het ontbreken van het betreffende relevante deel of de relevante delen het signaal niet meer kan worden gereconstrueerd. Overeenkomstig de oplossing volgens de uitvinding kan voor het veilig gecodeerd overdragen van informatiesignalen worden volstaan met het coderen van het betreffende relevante deel van het informatiesignaal, waarbij het resterende gedeelte ongecodeerd kan worden overgedragen.

Door het volgens een verdere uitvoeringsvorm van de uitvinding zodanig selecteren van het te coderen relevante deel van een informatiesignaal dat dit deel een relatief gering, bij voorkeur een zo gering mogelijk deel van de bandbreedte van het informatiesignaal in beslag neemt, kan er voor worden gezorgd dat de door het codeer- en decodeerproces veroorzaakte vertragingen in de signaaloverdracht minimaal zijn.

In bijvoorbeeld een gecodeerd digitaal videosignaal kunnen verschillende velden worden onderscheiden, bijvoorbeeld specifiek op de signaaloverdracht betrekkende hebbende velden waarmee, wanneer zij niet in het signaal aanwezig zijn, het onmogelijk is om de informatie-inhoud van het digitale videosignaal tot zich te nemen. Voorbeelden van dergelijke velden zijn bijvoorbeeld synchronisatievelden of het FEC-veld

in een "Digital Video Broadcasting" (DVB)-videosignaal. Deze velden beslaan slechts een relatief gering aantal bits van het totale videosignaal. De werkwijze volgens de uitvinding is in wezen bij alle digitale data-overdracht toepasbaar, omdat vrijwel elk data-overdrachtsprotocol bepaalde stuur-, controle- of andere gegevensvelden bezit welke noodzakelijk zijn om het betreffende signaal te kunnen reconstrueren. De werkwijze volgens de uitvinding is ook toepasbaar bij de overdracht van analoge signalen, waarbij in het algemeen ook door het afsplitsen van een relevant deel van het signaal het resterende deel onbruikbaar wordt.

In een communicatiesysteem dat verschillende transmissiekanalen omvat worden in een voorkeursuitvoeringsvorm van de uitvinding de gecodeerde relevante delen van informatiesignalen via een ander transmissiekanaal overgedragen dan de ongecodeerde restdelen. Hierdoor is het mogelijk om, in plaats van het afzonderlijk veilig coderen van de relevante delen, deze ook via een betreffend beveiligd transmissiekanaal over te dragen, zoals een transmissiekanaal waarop data middels de zogeheten "Code Division Multiple Access" (CDMA)-techniek gecodeerd worden overgedragen.

Het gebruik van CDMA-technieken garandeert een lage kans op onderschepping, zonder dat de betreffende relevante delen van informatiesignalen afzonderlijk moeten worden gecodeerd.

Een derde welke een betreffend informatiesignaal wil onderscheppen, dient derhalve in staat te zijn om het gecodeerde relevante deel te onderscheppen en het bijbehorende restdeel. Zelfs wanneer dit tot een resultaat zou lijden, dient er ook nog kennis te bestaan omtrent de wijze waarop de betreffende delen tot het oorspronkelijke informatiesignaal moeten worden gecombineerd. Derhalve geniet het de voorkeur om niet steeds eenzelfde relevant deel van een informatiesignaal af te splitsen en gecodeerd over te dragen maar, voor zover mogelijk, verschillende relevante signaaldelen te onderscheiden en van de over te dragen informatiesignalen afwisselend verschillende relevante delen te selecteren.

De uitvinding heeft tevens betrekking op een communicatiesysteem, omvattende codeermiddelen voor het in gecodeerde vorm veilig overdragen van informatiesignalen en decodeermiddelen voor het decoderen van overgedragen informatiesignalen, verder gekenmerkt door middelen voor het splitsen van een over te dragen informatiesignaal in

een voor verwerking van het signaal relevant deel en een restdeel, welke middelen werkzaam zijn gekoppeld met de codeermiddelen voor het in veilig gecodeerde vorm overdragen van het relevante deel van een informatiesignaal en met middelen voor het in ongecodeerde vorm overdragen van het restdeel van een informatiesignaal, waarbij de decodeermiddelen zijn ingericht voor het decoderen van een overgedragen relevant deel van een informatiesignaal en werkzaam zijn gekoppeld met middelen voor het tot een oorspronkelijk informatiesignaal reconstrueren van een gedecodeerd relevant deel en een overgedragen bijbehorend restdeel.

In de voorkeursuitvoeringsvorm van het communicatiesysteem volgens de uitvinding zijn de codeermiddelen ingericht voor het CDMA-gecodeerd overdragen van de relevante delen van een informatiesignalen.

De uitvinding heeft tevens betrekking op signaalsplitsmiddelen en signaalcombinatiemiddelen voor het respectievelijk splitsen en combineren van relevante delen en restdelen van een informatiesignaal, zoals boven beschreven.

De uitvinding wordt in het navolgende meer gedetailleerd beschreven en getoond in de bijgevoegde tekeningen, waarin:

fig. 1 schematisch de werkwijze volgens de uitvinding illustreert;

fig. 2 een vereenvoudigd blokschema van een "Direct Sequence" CDMA (DS-CDMA)-systeem toont;

fig. 3 een voorbeeldschema van een CATV-net toont, waarin de werkwijze volgens de uitvinding kan worden toegepast;

fig. 4 een vereenvoudigd blokschema van een eerste uitvoeringsvorm van een communicatiesysteem volgens de uitvinding toont, en

fig. 5 een vereenvoudigd blokschema van een voorkeursuitvoeringsvorm van een communicatiesysteem volgens de uitvinding toont.

Fig. 1 illustreert, in de vorm van een stroomdiagram, de werkwijze volgens de uitvinding, waarbij door middel van pijlen de bewerkingsvolgorde is geïllustreerd. Een informatiesignaal 1 wordt als eerste aan een splitsingsoperatie 2 onderworpen. Het informatiesignaal wordt hier gesplitst in een voor de signaalverwerking relevant deel 3 en een restdeel 4.

Het relevante deel kan uit één of meer delen van het informatiesignaal zijn opgebouwd, welke afzonderlijk of in combinatie noodzakelijk zijn voor de verdere verwerking van het informatiesignaal, dat wil zeggen zodanig dat samen met het restdeel een bruikbaar informatiesignaal wordt verkregen. Het relevante deel 3 kan dus zowel bestaan uit een gedeelte van de informatie-inhoud van het signaal en/of informatie voor het reconstrueren van het signaal, zoals synchronisatie en andere stuurinformatie. Het informatiesignaal kan daarbij bestaan uit zowel een digitaal als een analoog signaal.

In het geval dat een informatiesignaal verschillende voor de verwerking van het signaal relevante delen bezit, kan de splitsingsoperatie 2 zodanig worden uitgevoerd, dat van de arriverende informatiesignalen 1 telkens een selectie uit de relevante delen 3 kan worden gemaakt, zodanig dat van opeenvolgende informatiesignalen de relevante delen 3 en de restdelen 4 qua opbouw verschillend zijn. De wijze waarop de betreffende relevante delen 3 worden geselecteerd kan van te voren vastgelegd zijn of middels een kenmerk worden overgedragen.

Het geselecteerde relevante deel 3 wordt vervolgens aan een codeeroperatie 5 onderworpen. Deze codeeroperatie 5 heeft tot het doel het relevante deel te coderen voor veilige overdracht 6 over een transmissienet, zoals bijvoorbeeld een "point-to-multipoint" signaaldistributienet. Voorbeelden van dergelijke signaaldistributienetten zijn "Community Antenna TeleVision" (CATV)-netten en distributienetten voor elektrische energie zoals het elektriciteitsdistributienet in huizen, kantoren etc. en ook distributienetten voor elektrische tractie zoals in gebruik bij spoorweg-, tram- en trolleybusmaatschappijen.

Voor het coderen van het relevante deel zijn op zichzelf bekende coderingstechnieken bekend, welke met beveiligde codeer- en decodeersleutels werken zoals de "Rivest, Shamir, Aldehman (RSA) en "Data Encryption Standard" (DES) encryptie-algoritmes welke geen deel uitmaken van de onderhavige uitvinding. Voor een meer uitgebreide beschrijving van encryptie-algoritmes wordt verwezen naar het boek "Applied Cryptography", door Bruce Shneier, 2nd edition, John Wiley & Sons 1995.

Aan de ontvangende zijde wordt het overgedragen gecodeerde relevante deel 3 in een decodeeroperatie 7 gedecodeerd. Het restdeel 4 wordt na overdracht 8 aan de ontvangende zijde met het

gedecodeerde relevante deel gecombineerd 9, zodanig dat het aldus verkregen informatiesignaal 10 overeenkomt met het oorspronkelijk overgedragen informatiesignaal 1.

Overeenkomstig de uitvinding kan het restdeel 4 in ongecodeerde vorm worden overgedragen omdat het informatiesignaal 1 zodanig is gesplitst, dat het restdeel 4 op zichzelf onbruikbaar is. Onder ongecodeerde overdracht 8 wordt bedoeld dat het restdeel 4 niet wordt begrepen aan een vorm van encryptie of codering van de informatie waarbij het betreffende restdeel zonder kennis omtrent codeer- en/of decodeersleutels niet kan worden verwerkt. Uiteraard kan het restdeel 4 wel volgens een bekend protocol of bekende modulatietechniek worden overgedragen.

In plaats van het afzonderlijk coderen van relevante delen 3, kunnen de codeer-, overdracht- en decodeeroperaties 5, 6 en 7 worden uitgevoerd door het transmissiemedium waarover het relevante deel 3 wordt overgedragen. Dit is in het bijzonder van voordeel in een communicatiesysteem met verschillende transmissiekanalen, waarbij het relevante deel 3 van een informatiesignaal via een veilig gecodeerd transmissiekanaal wordt overgedragen en het restdeel 4 via een niet-beveiligd kanaal kan worden verzonden. In een voorkeursuitvoeringsvorm van de uitvinding wordt het relevante deel 3 overgedragen onder toepassing van de zogeheten "Code Division Multiple Access" (CDMA)-techniek.

CDMA of "Spread Spectrum" (SS) is een transmissietechniek waarbij de databits van een over te dragen digitaal signaal in een aantal elementen of chips worden gecodeerd, zodanig dat elk databit als een reeks van symbolen wordt overgedragen. Deze symbolen kunnen op zichzelf de logische waarde "1" of "0" aannemen of in het ritme van de betreffende reeks overgedragen frequentievariaties. In het eerste geval spreekt van "Direct Sequence CDMA" (DS-CDMA) en in het tweede geval van "Frequency Hopping CDMA" (FH-CDMA). In beide gevallen kan het overgedragen signaal weer worden gereconstrueerd indien de volgorde van de overgedragen chips of de frequenties bij de ontvanger bekend zijn. Afhankelijk van de omvang van de reeks, dat wil zeggen het aantal symbolen waarin het overgedragen bit wordt gecodeerd, zijn een veelvoud van onafhankelijke codes beschikbaar waardoor gelijktijdig verschillende gebruikers van eenzelfde transmissiekanaal gebruik kunnen maken. Alleen de gebruiker met de juiste code is in staat om de met deze code overgedragen databits te ontvangen.

Figuur 2 toont een vereenvoudigd blokschema van een DS-CDMA systeem met een transmissiekanaal 11, een zender 12 en een ontvanger 13. Het kanaal 11 kan een draadgebonden, optisch of draadloos communicatiekanaal zijn waaronder begrepen een radiokanaal, een infraroodkanaal en een ultrasoon-transmissiekanaal. In een CDMA-transmissiesysteem wordt door verschillende gebruikers j tegelijkertijd informatie over het transmissiekanaal 11 overgedragen, zoals gerepresenteerd middels een sommatieblok 16 waarbij een aantal van j = 1 tot en met N gebruikers 15 is verondersteld. Het totale signaal op het transmissiekanaal 11 wordt dan theoretisch gevormd door de som van een ruisbron 14 en de signalen van de gebruikers 15, zoals schematisch aangeduid door een sommator 17.

De zender 12 bestaat in wezen uit een modulator 18 met een ingang 19 waaraan over te dragen databits worden toegevoerd. De modulator 18 verwerkt de databits 19 tot geschikte signalen voor overdracht via het transmissiekanaal 11. De ontvanger 13 bezit een demodulator 20 met een uitgang 21 voor het afgeven van de overgedragen gedemoduleerde databits.

Voor transmissie volgens het DS-CDMA principe worden de van een zender 12 naar een ontvanger 13 door een gebruiker j over te dragen databits elk met een, door een codegenerator 22 opgewekte code $C_j^N(t)$ en een mengschakeling 23 in een aantal symbolen (chips) gecodeerd. Een logische "1" wordt bijvoorbeeld door de betreffende code zelf en een logische "0" wordt bijvoorbeeld door de inverse van de code gerepresenteerd. Naarmate de code langer is zal het over te dragen signaal meer en meer een ruissignaal benaderen, waardoor detectie zonder kennis van de betreffende code nagenoeg onmogelijk is.

Het op deze wijze in de frequentie gespreide DS-CDMA signaal van de gebruiker j kan na een transmissievertragingstijd τ_j bij de ontvanger 13 via eenzelfde codegenerator 22 echter met de code $C_j^N(t)$ en mengschakeling 24 worden gereconstrueerd, mits de code bekend is waarmee de databits voor de j-de gebruiker zijn gecodeerd.

Voor een meer gedetailleerde uitleg van CDMA- en Spread Spectrum-technieken wordt verwezen naar op dit vakgebied bekende literatuur, waaronder de boeken "Spread Spectrum Systems with Applications", door R.C. Dixon, John Wiley & Sons, Inc., 1994 en "CDMA, Principles

of Spread Spectrum Communications", door A.J. Viterbi, Addison-Wesley Publishing Company. In de werkwijze volgens de voorkeursuitvoeringsvorm van de uitvinding wordt derhalve de vereiste veilige codering van het relevante deel van een informatiesignaal door het betreffende transmissiekanaal verzorgt waarover de overdracht plaatsvindt. Het gebruik van CDMA-technieken garandeert een lage kans op onderschepping.

Omdat ook het restdeel via een gemeenschappelijk of een veelheid van gemeenschappelijke transmissiekanalen van een communicatiesysteem wordt overgedragen, zal het zelfs bij onderscheppen van een gecodeerd relevant deel 3 nog bijzonder moeilijk zijn om het bijbehorende restdeel 4 te selecteren en wanneer het relevante deel 3 afwisselend uit een veelvoud van relevante signaaldelen wordt geselecteerd, zal het eveneens problematisch zijn om de beide delen tot het oorspronkelijke informatiesignaal te combineren.

Het relevante deel 3 wordt, in het geval van een relatief breedbandig signaal, zoals een videosignaal, zodanig gekozen, dat het slechts een relatief gering gedeelte van de totale signaalbandbreedte in beslag neemt. In een praktische situatie wordt het relevante deel 3 bij voorkeur zodanig gekozen, dat het via een 64 kb/s transmissiekanaal kan worden overgedragen, terwijl het restdeel 4, bijvoorbeeld in het geval van een videosignaal, via een breedbandig transmissiekanaal in de ordegrootte van 2 Mb/s of hoger wordt overgedragen. Het zal duidelijk zijn dat bij een overdrachtstechniek waarbij meerdere gebruikers tegelijkertijd op eenzelfde kanaal actief kunnen zijn, zoals CDMA, maar ook volgens de zogeheten "Time Division Multiple Access" (TDMA)-techniek werkende transmissiekanalen, met de werkwijze volgens de uitvinding op veilige wijze informatie in een distributienet kan worden overgedragen.

Een voorbeeld van een point-to-multipoint datadistributienet is het reeds eerder genoemde CATV-net, waarvan fig. 3 een voorbeeldsuitvoeringsvorm toont. In de getoonde netstructuur 25 wordt informatie vanaf een hoofdstation 26 naar eindaansluitpunten 27 overgedragen. Tussen het hoofdstation 26 en de eindaansluitpunten 27 zijn diverse bi-directionele versterkers 28, 29, 30 geschakeld, voor het opheffen van transmissieverliezen in het net 25, dat gebruikelijk uit coaxiale kabel 32 is opgebouwd.

In de getoonde uitvoeringsvorm zijn de versterkers 28 in de vorm van een zogeheten ringnet op het hoofdstation 26 aangesloten, waarbij de van een versterker 28 ontvangen signalen in een districtstation 31 verder via een groepsversterker 29 worden gedistribueerd. De gebruikers of eindaansluitpunten 27 zijn stervormig op een eindversterker 30 aangesloten die signalen van een groepsversterker 29 ontvangt.

In Nederlands CATV-netten zijn de versterkers 28, 29 en 30 in het algemeen zodanig ingericht, dat zij signalen vanaf het hoofdstation 26 naar de eindaansluitpunten 27 in een brede frequentieband van circa 50 MHz tot boven 750 MHz doorlaten. De transmissierichting vanaf het hoofdstation 26 naar de eindaansluitpunten 27 wordt ook wel met "stroomafwaarts" aangeduid. In de andere richting, dat wil zeggen vanaf de eindaansluitpunten 27 naar het hoofdstation 26, ook wel "stroomopwaarts" genoemd, is een transmissiefrequentieband van 5 MHz tot circa 50 MHz beschikbaar. Gestreefd wordt naar een volledig passieve transmissiefrequentieband in het frequentiegebied tot ca. 70 MHz, dat wil zeggen zonder versterkers.

Onder meer afhankelijk van de lengte van de code waarmee databits in CDMA worden gecodeerd, kunnen meer dan 100 gebruikers gelijktijdig op eenzelfde transmissiekanaal informatie overdragen.

Fig. 4 toont een vereenvoudigd blokschema van een eerste uitvoeringsvorm van een communicatiesysteem voor het gedeeltelijk gecodeerd overdragen van informatiesignalen volgens de uitvinding. Een over te dragen informatiesignaal wordt aan een ingang 33 van signaalsplitsmiddelen 34 toegevoerd, welke aan een eerste uitgang 35 de relevante signaaldelen en aan een uitgang 36 het restdeel van het over te dragen informatiesignaal afgeven.

Het relevante deel 35 wordt in codeermiddelen 37 veilig gecodeerd volgens een op zichzelf bekende coderingstechniek en aan een uitgang 38 afgegeven. De signalen aan de uitgangen 36 en 38 worden in een multiplexer 39 tot een voor overdracht via een zender 48 en transmissiekanaal 40 geschikt signaal gecombineerd. Het door een ontvanger 49 ontvangen overgedragen signaal wordt in een demultiplexer 41 weer gescheiden in een restdeel en het gecodeerde relevante deel, respectievelijk afgegeven aan uitgangen 42 en 43. Het gecodeerde signaal op de uitgang 43 wordt aan decodeermiddelen 44 toegevoerd en het aan een uitgang 45 van de

decodeermiddelen 44 afgegeven gedecodeerde signaal wordt samen met het op de uitgang 42 van de demultiplexer 41 beschikbare restdeel in signaalcombinatiemiddelen 46 tot een informatiesignaal gecombineerd, dat vervolgens op een uitgang 47 van de signaalcombinatiemiddelen 46 beschikbaar is.

Fig. 5 toont een voorkeursuitvoeringsvorm van een communicatiesysteem volgens de uitvinding, waarbij de signalen op de uitgangen 35 en 36 van de signaalsplitsmiddelen 34 via afzonderlijke transmissiekanalen 50, 51 worden overgedragen.

Het kanaal 51, waarover het restdeel van een informatiesignaal 33 wordt overgedragen, kan van het type zijn waarover informatie op ongecodeerde, dat wil zeggen niet versleutelde of anderszins beveiligde wijze, wordt overgedragen via zend- en ontvangmiddelen 52, 53. Uiteraard kan het restdeel wel volgens een geschikt of voorgeschreven transmissieprotocol tot een voor overdracht via het transmissiekanaal 51 geschikt formaat zijn verwerkt.

Overeenkomstig de in fig. 3 geïllustreerde uitvoeringsvorm, kan het relevante deel van het informatiesignaal 33 aan de uitgang 35 van de signaalsplitsmiddelen 34 op geschikte wijze gecodeerd 54, verzonden 55, ontvangen 56 en gedecodeerd 57 worden, onder toepassing van een daartoe geschikt transmissieprotocol en codeeralgoritme.

In de voorkeursuitvoeringsvorm van de uitvinding wordt het relevante deel van een informatiesignaal 33 via een veilig transmissiekanaal overgedragen, in het bijzonder een CDMA-gecodeerd transmissiekanaal, zoals aangegeven met de onderbroken lijnen 58 in fig. 5. De codeer- en zendmiddelen 54, 55 en de ontvang- en decodeermiddelen 56, 57 zijn ingericht voor CDMA-overdracht zoals besproken aan de hand van fig. 2.

De transmissiekanalen 50 en 51 kunnen deel uitmaken van een meer omvangrijke communicatiesysteem zoals een CATV-net waarbij meerdere gebruikers gelijktijdig over een informatiekanaal informatie overdragen. In het bijzonder bij CDMA-data-overdracht kunnen de relevante delen van verschillende gebruikers gelijktijdig over het transmissiekanaal 50 op een veilige wijze worden overgedragen zodanig, dat alleen de eindgebruiker welke beschikt over de juiste sleutel waarmee een betreffend relevant deel is gecodeerd de informatie uit de veelheid van relevante delen van verschillende gebruikers kan terugwinnen.

Voor het combineren van een bijbehorend relevant deel en een restdeel kan aan elk van de delen een specifieker kenmerk worden toegevoegd, zoals een bestemmingsnummer of gebruikersnummer en een volgnummer, zodanig dat de signaalcommunicatiemiddelen 46 de betreffende signaaldelen tot een uiteindelijk compleet informatiesignaal aan de uitgang 47 kunnen combineren.

In plaats van CDMA-transmissie kan ook elke andere vorm van veilige transmissie voor het doel van de uitvinding worden toegepast, zoals bijvoorbeeld transmissie in versleutelde vorm middels een "Time Division Multiple Access" (TDMA)-transmissieprotocol overeenkomstig het "Global Systems voor Mobile Communications" (GSM) of de "Digital Enhanced Cordless Telecommunications" (DECT)-standaard waarbij de informatie standaard in gecodeerde of versleutelde vorm wordt overgedragen.

Hoewel in de figuren 4 en 5 een communicatiesysteem voor simplex-overdracht (d.w.z. éénrichtingsverkeer) is getoond, zal het voor een deskundige geen toelichting behoeven dat de de uitvinding ook voor duplex-overdracht (d.w.z. voor tweerichtingsverkeer) geschikt is.

Conclusies

1. Werkwijze voor het in een communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken, met het kenmerk, dat een informatiesignaal wordt gesplitst in een voor verwerking van het signaal relevant deel en een restdeel, waarbij het relevante deel in een veilig gecodeerde vorm en het restdeel in ongecodeerde vorm via het communicatiesysteem worden overgedragen en dat een overgedragen relevant deel van een informatiesignaal wordt gedecodeerd en met een bijbehorend overgedragen restdeel tot het oorspronkelijke informatiesignaal wordt gereconstrueerd.

2. Werkwijze volgens conclusie 1, met het kenmerk, dat het te coderen relevante deel van het informatiesignaal zodanig wordt geselecteerd dat dit een relatief gering deel van de bandbreedte van het informatiesignaal in beslag neemt.

3. Werkwijze volgens conclusie 1 of 2, met het kenmerk, dat het communicatiesysteem verschillende transmissiekanalen omvat, waarbij het gecodeerde relevante deel en het ongecodeerde restdeel van het informatiesignaal elk via verschillende transmissiekanalen worden overgedragen.

4. Werkwijze volgens conclusie 1, 2 of 3, met het kenmerk, dat het te coderen relevante deel van het informatiesignaal onder toepassing van "Code Division Multiple Access" (CDMA)-techniek gecodeerd wordt overgedragen.

5. Werkwijze volgens conclusie 1, 2, 3 of 4, met het kenmerk, dat het communicatiesysteem een "point-to-multipoint" signaaldistributienet omvat, waarbij verschillende gebruikers gelijktijdig informatiesignalen kunnen ontvangen en/of verzenden, waaronder begrepen "Community Antenna TeleVision" (CATV)-netten en distributienetten voor elektrische energie.

6. Communicatiesysteem, omvattende codeermiddelen voor het in gecodeerde vorm veilig overdragen van informatiesignalen en decodeermiddelen voor het decoderen van overgedragen informatiesignalen, verder gekenmerkt door middelen voor het splitsen van een over te dragen informatiesignaal in een voor verwerking van het signaal relevant deel en een restdeel, welke middelen werkzaam zijn gekoppeld met de codeermid-

delen voor het in veilig gecodeerde vorm overdragen van het relevante deel van een informatiesignaal en met middelen voor het in ongecodeerde vorm overdragen van het restdeel van een informatiesignaal, waarbij de decodeermiddelen zijn ingericht voor het decoderen van een overgedragen relevant deel van een informatiesignaal en werkzaam zijn gekoppeld met middelen voor het tot een oorspronkelijk informatiesignaal reconstrueren van een gedecodeerd relevant deel en een overgedragen bijbehorend restdeel.

7. Communicatiesysteem volgens conclusie 6, met het kenmerk, dat de middelen voor het splitsen van het informatiesignaal zijn ingericht voor het selecteren van een relevant deel van het informatiesignaal met een relatief geringe bandbreedte ten opzichte van de bandbreedte van het totale informatiesignaal.

8. Communicatiesysteem volgens conclusie 6 of 7, met het kenmerk, dat het communicatiesysteem verschillende transmissiekanalen omvat voor het via een verschillend transmissiekanaal overdragen van het relevante deel en het restdeel van een informatiesignaal.

9. Communicatiesysteem volgens conclusie 6, 7 of 8, met het kenmerk, dat de codeermiddelen zijn ingericht voor het in "Code Division Multiple Access" (CDMA)-gecodeerd overdragen van het relevante deel van een informatiesignaal.

10. Signaalsplitsmiddelen voor gebruik in een communicatiesysteem volgens conclusie 6, 7, 8 of 9, voor het splitsen van een over te dragen informatiesignaal, met het kenmerk, dat de signaalsplitsmiddelen zijn ingericht voor het, van het informatiesignaal afsplitsen van een voor de verwerking van het signaal relevant deel.

11. Signaalcombinatiemiddelen voor gebruik in een communicatiesysteem volgens conclusie 6, 7, 8 of 9, met het kenmerk, dat de signaalcombinatiemiddelen zijn ingericht voor het tot een totaal informatiesignaal combineren van een gedecodeerd overgedragen relevant deel en een overgedragen bijbehorend restdeel van een informatiesignaal.

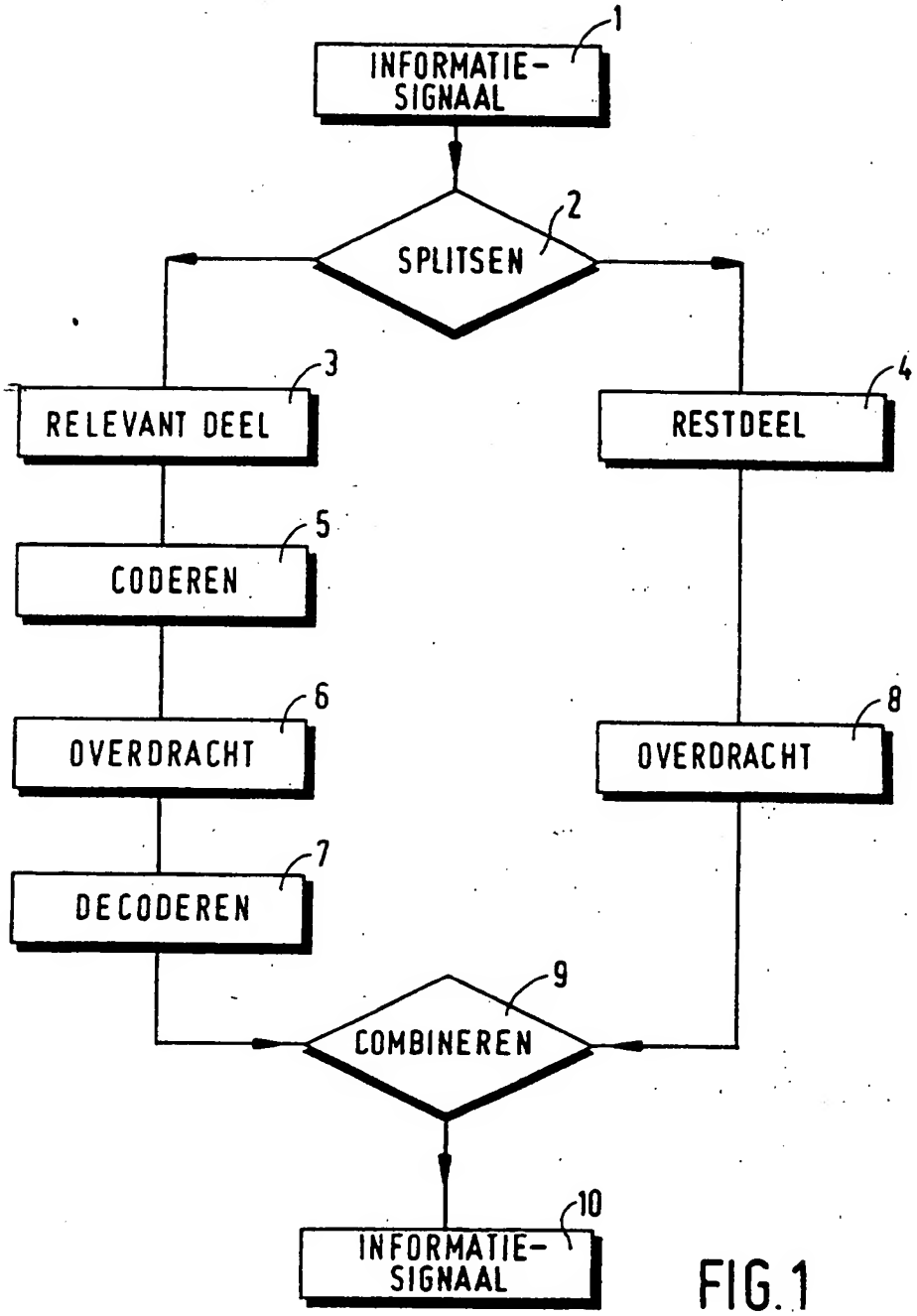

FIG.1

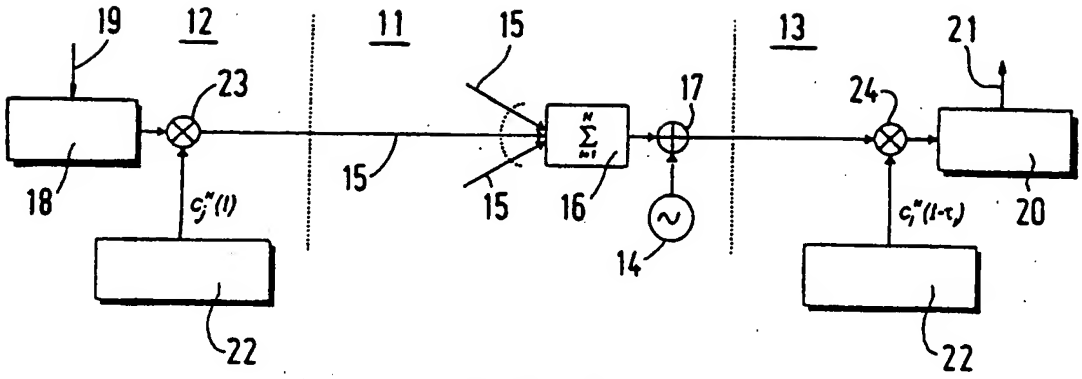

FIG. 2

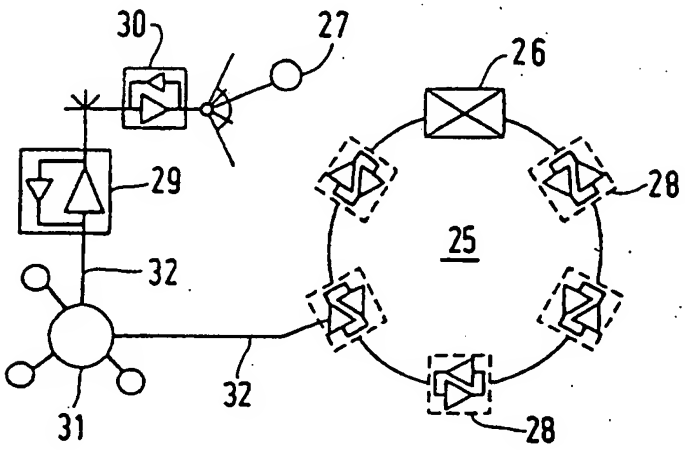

FIG. 3

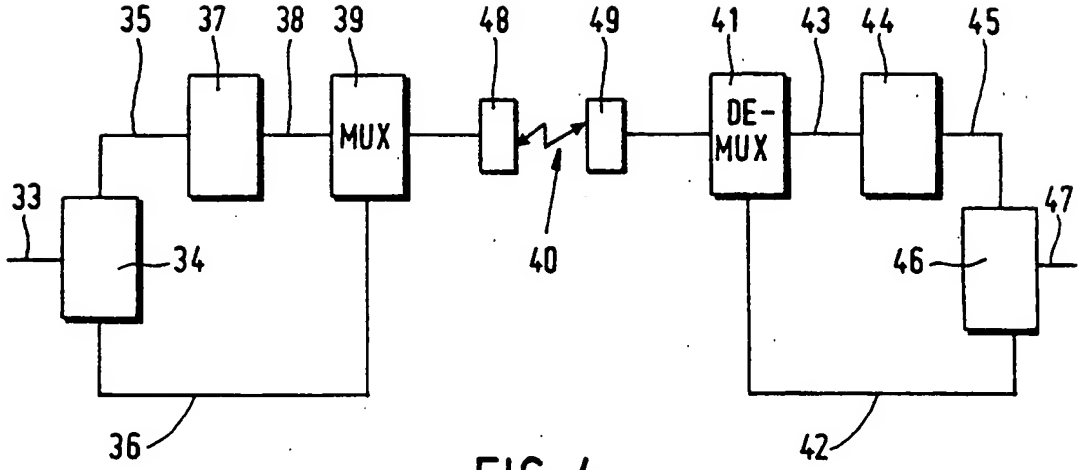

FIG. 4

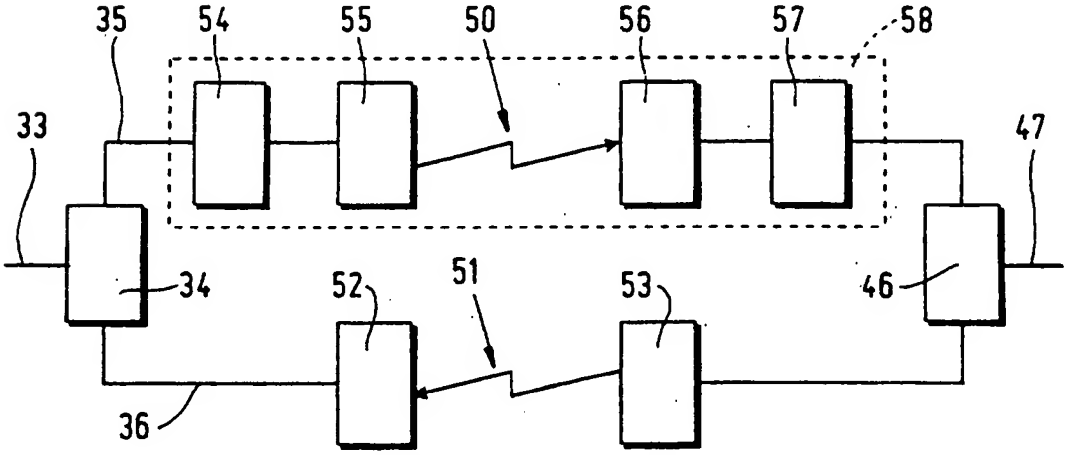

FIG. 5

SAMENWERKINGSVERDRAG (PCT)

RAPPORT BETREFFENDE

NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFIKATIE VAN DE NATIONALE AANVRAGE	Kenmerk van de aanvrager of van de gemachtigde
	37739/JD/jr
Nederlandse aanvrage nr.	Indieningsdatum
1005523	13 maart 1997
	Ingeroepen voorrangsdatum

Aanvrager (Naam)

TECHNISCHE UNIVERSITEIT EINDHOVEN

Datum van het verzoek voor een onderzoek van internationaal type	Door de Instantie voor Internationaal Onderzoek (ISA) aan het verzoek voor een onderzoek van internationaal type toegekend nr.
--	SN 28858 NL

I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)

Volgens de Internationale classificatie (IPC)

Int. Cl.^{6}: H 04 N 7/167, H 04 N 7/26

II. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie

Classificatiesysteem	Classificatiesymbolen
Int. Cl.^{6}	H 04 N

Onderzochte andere documentatie dan de minimum documentatie voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

III. ☐ GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES (opmerkingen op aanvullingsblad)

IV. ☐ GEBREK AAN EENHEID VAN UITVINDING (opmerkingen op aanvullingsblad)

20

BNSDOCID: <NL___1005523C2_I_>

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1005523

A. CLASSIFICATIE VAN HET ONDERWERP
IPC 6 H04N7/167 H04N7/26

Volgens de Internationale Classificatie van octrooien (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie (classificatie gevolgd door classificatiesymbolen)
IPC 6 H04N

Onderzochte andere documentatie dan de minimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie *	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	TIHAO CHIANG ET AL: "HIERARCHICAL CODING OF DIGITAL TELEVISION" IEEE COMMUNICATIONS MAGAZINE, deel 32, nr. 5, 1 Mei 1994, bladzijden 38-45, XP000451094 zie bladzijde 41, rechter kolom, regel 40 - bladzijde 43, linker kolom, regel 23 zie figuur 3 ---	1,2,5-7, 10,11
A	DE 44 25 197 A (DEUTSCHE BUNDESPOST TELEKOM) 25 Januari 1996 zie kolom 1, regel 7 - kolom 4, regel 42 zie figuren 1,2 -----	1-11

☐ Verdere documenten worden vermeld in het vervolg van vak C.

☒ Leden van dezelfde octrooifamilie zijn vermeld in een bijlage

* Speciale categorieën van aangehaalde documenten

"A" document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang

"E" eerder document, maar gepubliceerd op de datum van indiening of daarna

"L" document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publikatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven

"O" document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel

"P" document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang

"T" later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvrage, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt

"X" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten

"Y" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt

"&" document dat deel uitmaakt van dezelfde octrooifamilie

1

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid	Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type
2 December 1997	

Naam en adres van de instantie	De bevoegde ambtenaar
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Van der Zaal, R

Formulier PCT/ISA/201 (tweede blad) (juli 1992)

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1005523

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
DE 4425197 A	25-01-96	GEEN	

Formulier PCT/ISA/201 (vervolgblad octrooifamilie) (juli 1992)

P ENT COOPERATION TREATY

RECEIVED

MAR 2 8 2001

PCT

BROBECK

From the INTERNATIONAL SEARCHING AUTHORITY

INVITATION TO PAY ADDITIONAL FEES

(PCT Article 17(3)(a) and Rule 40.2)

DOCKETED

Add'l Fees Due

16 Apr / 29 Apr 2001

To:
BAKER BOTTS L.L.P.
Attn. CHAPMAN, Floyd B.
THE WARMER
1299 PENNSYLVANIA AVENUE, N.W.
WASSHINGTON, D.C. 20004
UNITED STATES OF AMERICA

Date of mailing (day/month/year): 15/03/2001

Applicant's or agent's file reference: 066358.0106 031890.0007

PAYMENT DUE within 45 ~~months~~/days from the above date of mailing

International application No.: PCT/US 00/18411

International filing date (day/month/year): 05/07/2000

Applicant: MOSKOWITZ, Scott A.

1. This International Searching Authority

(i) considers that there are 2 (number of) inventions claimed in the international application covered by the claims indicated ~~below~~/on the extra sheet:

and it considers that the international application does not comply with the requirements of unity of invention (Rules 13.1, 13.2 and 13.3) for the reasons indicated ~~below~~/on the extra sheet:

(ii) [X] has carried out a partial international search (see Annex) [ ] will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:
1-5, 26-29

(iii) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid

2. The applicant is hereby **invited**, within the time limit indicated above, to pay the amount indicated below:

EUR 945,00 (Fee per additional invention) x 1 (number of additional inventions) = EUR 945,00 (total amount of additional fees)

Or, _____ x _____ = _____

The applicant is informed that, according to Rule 40.2(c), **the payment of any additional fee may be made under protest**, i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive.

3. [ ] Claim(s) Nos. _____ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

Name and mailing address of the International Searching Authority:
European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer: Marja Brouwers

Form PCT/ISA/206 (July 1992)

'ent Family Annex

Information on patent family members

Inte ional Application No
PCT/US 00/18411

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
NL 1005523 C	15-09-1998	NONE	
WO 9744736 A	27-11-1997	AU 3206397 A	09-12-1997
EP 0649261 A	19-04-1995	JP 7115638 A	02-05-1995
		US 5933499 A	03-08-1999
US 5974141 A	26-10-1999	US 6076077 A	13-06-2000
		US 6002772 A	14-12-1999
		US 6097818 A	01-08-2000

Annex Form PCT/ISA/206
COMMUNICATION RELATING TO THE RESULTS OF THE PARTIAL INTERNATIONAL SEARCH

International Application No
PCT/US 00/18411

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
1-5, 26-29
2. This communication is not the international search report which will be established according to Article 18 and Rule 43.
3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.
4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NL 1 005 523 C (EINDHOVEN TECH HOCHSCHULE) 15 September 1998 (1998-09-15) abstract; figure 4 page 1, line 35 -page 3, line 9 page 9, line 21 -page 10, line 5	1,2, 26-29
X	WO 97 44736 A (APPLE COMPUTER) 27 November 1997 (1997-11-27) abstract; figures 2A,2B,2C,3 page 2, line 35 -page 3, line 27 page 9, line 10 -page 11, line 28	1,2
Y		3,4
Y	EP 0 649 261 A (CANON KK) 19 April 1995 (1995-04-19) page 3, line 53 -page 4, line 5 page 7, line 18 - line 23	3,4
A	US 5 974 141 A (SAITO MAKOTO) 26 October 1999 (1999-10-26) abstract; figures 4A-4G column 8, line 24 - line 67	5,26

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Form PCT/ISA/206 (Annex, first sheet) (July 1992)

INVITATION TO PAY ADDITIONAL FEES

International application No.
PCT/US 00/18411

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-5, 26-29

   Protecting the distribution of digital data to be used with a digital player charachterized by encrypting format information and allowing low quality play back in case of lack of decrypting key.

2. Claims: 6-25

   Digital signal encrypting technique combining transfer functions with predetermined key creation.

This finding is based on the following reasons.

The prior art has been identified as NL1005523 (D1). This document shows a method for protecting the distribution of digital information, the digital information including two subparts, a digital sample and format information, comprising the steps of: identifying and separating the two subparts; encoding the format information subpart using a key; recombining the encoded first subpart with the un-encoded second subpart, generating in this way an encoded version of the digital information. A predetermined key corresponding to the encoding key is then required for the decryption of the format information. All the features which form the subject matter of claims 1 and 2 are then disclosed by D1 (see following passages: abstract; page 1, line 35 - page 3, line 9; page 9, line 21 - page 10, line 5; fig. 4)

From the comparison between D1 and the 1st invention (see claim 3) the following technical featuree can be seen to make a contribution over this prior art (in the sense of PCT rule 13.2):
- the digital information is configured to be used with a digital player and the information output from said digital player has a degraded quality unless it is provided with a predetermined key (Special Technical Features 1, STF1).
From these STF1 the objective problem to be solved can be summarized as:
- permitting preview of distributed digital information

From the comparison between D1 and the 2nd invention (see claim 6) the following feature can be seen to make a contribution over the same prior art:
- using a transfer function-based mask set for creating a key to manipulate data at the inherent granularity of the file format of a digital sample (STF2).
From this STF2 the objective problem to be solved can be summarized as:
- improving the security of techniques for data protection

The above analysis shows that inventions 1 and 2 do not have same or similar Special Technical Features. Furthermore, a comparison of the objective problem 1 with the objective problem 2, both seen in the light of the description and the drawings of the present application, indicates that there is no technical correspondence between these problems nor do they show any corresponding technical effect.

As a result, inventions 1 and 2 fail to demonstrate a single general inventive concept as required by PCT rule 13.1.